ATM Àrea de Barcelona
Autoritat del Transport Metropolità

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

Pliego de Prescripciones Técnicas para la contratación mediante procedimiento abierto sujeto a regulación armonizada los servicios de:

Oficina de Ciberseguridad ATM

(Exp. C-33/2023)

Agosto 2024

Next Generation Catalunya

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

ÍNDICE

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

Número d'expedient: C-33/2023

El contenido de estas prescripciones técnicas deriva del proyecto *Implantación del proyecto T-mobilitat (refuerzo de ciberseguridad)* que se encuentra dentro del componente 6 inversión 4: *"Digitalización de los servicios administrativos que se prestan por parte de las Comunidades Autónomas y las ciudades de Ceuta y Melilla, en relación con el transporte de mercancías y de viajeros por carretera o ferrocarril de su competencia. En este ámbito se incluirán los proyectos digitales necesarios para poder ofrecer un servicio de transporte a la demanda, en el ámbito competencial de las Comunidades Autónomas y las ciudades de Ceuta y Melilla*" (dentro de la submedida 15 de la inversión 4 del PRTR) y Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo de 12 de febrero de 2021, por el que se establece el mecanismo de Recuperación y Resiliencia, en el marco del Plan de Recuperación, Transformación y Resiliencia – Financiado por la UE - NextGenerationEU.

Este proyecto se aprobó en el marco del Plan de Recuperación, Transformación y Resiliencia, que incluye las actuaciones en el marco del componente 6, derivadas del Acuerdo de la Conferencia Nacional de Transportes de 20 de junio de 2022, por la que se modifica la resolución de 24 de noviembre de 2021, la cual formalizaba los compromisos financieros con la Comunidad Autónoma de Catalunya para el ejercicio 2021 para la financiación de actuaciones en el marco del componente 6, derivados del acuerdo de la conferencia nacional de transportes de 5 de noviembre de 2021 por el que se fijan los criterios de distribución territorial de créditos presupuestarios de los ejercicios 2021 y 2022, así como la distribución correspondiente al ejercicio de 2021, para la financiación de actuaciones de inversión en el marco de los componentes 1 "plan de choque de movilidad sostenible, segura y conectada en entornos urbanos y metropolitanos" y 6 "movilidad sostenible, segura y conectada" del plan de recuperación, transformación y resiliencia.

Entre las actuaciones objeto de financiación contenidas en la resolución de 24 de noviembre de 2021 de la secretaría de Estado de Transportes, Movilidad y Agenda Urbana se encuentra la de implementación de mejoras de ciberseguridad en el proyecto T-movilidad, que está incluida en el componente 6 "movilidad sostenible, segura y conectada".

Dentro del alcance de este proyecto se encuentra la contratación relativa a los servicios de la "Oficina de Ciberseguridad ATM" objeto de licitación de acuerdo con lo previsto en los presentes pliegos.

Con la mera presentación de su oferta, la empresa licitadora acepta las prescripciones técnicas establecidas en este pliego.

Cualquier propuesta que no se ajuste a los requerimientos mínimos establecidos en este pliego quedará automáticamente excluida de la licitación.

1. Contexto

La Autoritat del Transport Metropolità de l'Àrea de Barcelona (en adelante ATM) es un consorcio interadministrativo de carácter voluntario, creado en 1997. Actualmente, las administraciones consorciadas son la Generalitat de Catalunya (51%) y administraciones locales (49%), compuestas por el Ajuntament de Barcelona, el Área Metropolitana de Barcelona (anteriormente denominada Entitat Metropolitana del Transport) y la Associació de Municipis per la Mobilitat i el Transport Urbà (AMTU), al que se pueden adherir todas las administraciones titulares de servicios públicos de transporte colectivo, que pertenezcan al ámbito formado por las comarcas de L'Alt Penedès, L'Anoia, El Bages, El Baix Llobregat, El

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

Barcelonès, El Berguedà, El Garraf, El Maresme, Osona, El Vallès Occidental y El Vallès Oriental. Además, la Administración General del Estado está presente en los órganos de gobierno de la ATM en calidad de observador.

El Área de Sistemas e Innovación tiene encomendadas, entre otras, la gestión de las políticas de seguridad informática y de protección de datos, la de los sistemas de seguridad en red y la de los sistemas corporativos de autenticación de usuarios. Esta Área administra una infraestructura de comunicaciones y servidores que proporciona el soporte sobre el que se implementan las aplicaciones corporativas, se distribuye la información de sus servicios y se prestan los servicios telemáticos a los ciudadanos. En consonancia con el principio básico de "Líneas de defensa" establecido en el Real Decreto 311/2022 del 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), para asegurar estas comunicaciones, es necesario orientar la estrategia de seguridad hacia una solución de arquitectura multicapa, consistente en introducir múltiples capas de seguridad que permitan reducir la probabilidad de que los sistemas de información se vean comprometidos y minimizar el impacto si la situación de riesgo llega a materializarse.

Teniendo en cuenta la evolución y expansión de los ciberataques durante estos últimos años, el refuerzo de la protección de la ciberseguridad se considera necesario para mitigar en todo lo posible los efectos de estos ataques.

El aumento de herramientas de ciberseguridad y su explotación, el control de los datos de las organizaciones, así como la necesidad de adaptarse a las diferentes normativas como el ENS o a estándares como ISO, implica a la ATM la necesidad de disponer de una Oficina de Ciberseguridad que en coordinación con el CISO, pueda establecer el marco ideal en la gestión de la ciberseguridad y la protección de los datos.

En el presente Pliego de Prescripciones Técnicas se describen las necesidades al respecto.

2. Hitos y objetivos

Que la Unión Europea (UE) creó los Fondos Next Generation EU (en adelante, NGEU) para ayudar a mitigar el impacto económico y social de la pandemia de la COVID-19 y hacer que las economías y sociedades europeas fueran más sostenibles y resilientes, aprobados mediante el Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo de 12 de febrero de 2021 por el que se establece el Mecanismo de Recuperación y Resiliencia (en adelante, MRR).

Que uno de los objetivos de la Componente 6 "movilidad sostenible, segura y conectada" del MRR es la "Digitalización de los servicios administrativos que se prestan por parte de las comunidades autónomas y las ciudades de Ceuta y Melilla, en relación con el transporte de mercancías y de viajeros por carretera o ferrocarril de su competencia. En este ámbito se incluirán los proyectos digitales necesarios para poder ofrecer un servicio de transporte a la demanda, en el ámbito competencial de las Comunidades Autónomas y las ciudades de Ceuta y Melilla (dentro de la submedida 15 de la inversión 4 del PRTR).

Se establecen las siguientes metas y objetivos asociadas a la ejecución del contrato:

1: Se prevé la finalización del proyecto antes del 20 de junio del 2026.

El adjudicatario deberá facilitar, en tiempo y forma, la información que le sea requerida para acreditar el cumplimiento de las metas y objetivos fijados. La falta de entrega de esta información o su entrega incumplida fuera de plazo o sin respetar las especificaciones de este

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

Pliego y resto de prescripciones técnicas del contrato, podrá ser considerada causa de incumplimiento.

En caso de incumplimiento por causa imputable al Adjudicatario de las metas y objetivos establecidos, dará lugar a la imposición de las penalizaciones previstas en la cláusula 22 del Pliego de Cláusulas Administrativas.

El incumplimiento de las metas y objetivos establecidos, dado su carácter de condición esencial de ejecución es causa de resolución del contrato de acuerdo con la cláusula 39 del Pliego.

En cuanto a los mecanismos para el control de las metas y objetivos, la empresa adjudicataria deberá colaborar en todo aquello que le sea requerido para la verificación, seguimiento y cumplimiento de las obligaciones derivadas de la normativa interna y europea fijadas por el Mecanismo de Recuperación y Resiliencia de la UE que se establezcan.

3. Objecto del contrato

El objeto de este contrato es la implementación de una Oficina de Ciberseguridad de la ATM, que estará en dependencia del CISO e integrada en el Área de Sistemas e Innovación.

Teniendo en cuenta la evolución y expansión de los ciberataques durante estos últimos años, el refuerzo de la protección de la ciberseguridad se considera necesario para mitigar en todo lo posible los efectos de estos ataques.

Con este objetivo, la ATM requiere disponer de una Oficina de Ciberseguridad que en coordinación con el CISO, pueda establecer el marco ideal en la gestión de la ciberseguridad y la protección de los datos, que podrá dar respuesta y coordinar la necesidad de aumentar las herramientas de ciberseguridad y su explotación, el control de los datos de las organizaciones, así como la necesidad de adaptarse a las diferentes normativas como el ENS o a estándares como ISO.

Las organizaciones se han tenido que adaptar a las normativas vigentes, GDPR, ENS. En paralelo, la complejidad de los órganos de gobierno de la ciberseguridad en las organizaciones también se ha tenido que adaptar.

Al respecto, la ATM dispone de la figura de un servicio de CISO, pero ahora se cree necesario aumentar la capacidad de la gestión de la ciberseguridad con la configuración de la Oficina de Ciberseguridad ATM, que en coordinación con el CISO e integrada en el Área de Sistemas e Innovación, pueda establecer el marco ideal en la gestión de la ciberseguridad y la protección de los datos.

Por estas razones se considera necesario la contratación de la integración de diferentes roles en la Oficina de Ciberseguridad de la ATM: un rol de analista técnico de ciberseguridad, un rol de analista técnico de datos, un rol de gestor documental de ciberseguridad y un rol de coordinador de la Oficina de Ciberseguridad.

4. Actividades y funciones de la empresa adjudicataria

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

La prestación regulada en este pliego debe ajustarse, a los requisitos técnicos especificados en este Pliego, sin perjuicio de los parámetros que deben valorarse mediante los criterios de adjudicación establecidos.

La empresa contratista debe disponer de los suficientes medios técnicos, materiales cualitativos y personales para desarrollar las tareas objeto del correspondiente contrato.

La prestación del servicio deberá cumplir con los parámetros de calidad y seguridad establecidos por la ATM, la legislación vigente y las principales normas y buenas prácticas aplicables a las tecnologías de la información y la comunicación para garantizar la confidencialidad, disponibilidad e integridad de la información a la que pueda tener acceso el adjudicatario en virtud del contrato.

Durante la prestación del servicio, el adjudicatario, juntamente con la ATM, definirán las medidas técnicas de seguridad más apropiadas para el servicio de acuerdo con los análisis de riesgos que se lleven a cabo a tal efecto en caso de que así se requiera.

La oferta que presente la empresa licitadora deberá abarcar la totalidad de la prestación de servicios y realización de las tareas especificadas en el presente pliego y en el Pliego de Cláusulas Administrativas Particulares, siendo todas ellas obligatorias para la admisión de las propuestas.

A continuación se describen las tareas a realizar por parte de cada uno de los perfiles que compondrán la oficina de Ciberseguridad:

4.1. Analista técnico de ciberseguridad

Este perfil debe llevar a cabo el control de las herramientas de ciberseguridad de la ATM y apoyo en la validación del marco normativo.

Las actividades y funciones a realizar por este perfil, a título enunciativo que no limitativo, son los siguientes:

- Asegurar la disponibilidad en estado óptimo y alcance de las herramientas
- Asegurar la monitorización, tratamiento y escalado de las alertas
- Realizar informes y cuadros de mando del estado y actividad de las herramientas
- Proponer y participar en la incorporación de nuevas herramientas
- Apoyar a las demás áreas de la oficina de ciberseguridad para validar los procedimientos operativos de la explotación de los sistemas, así como de las evidencias aportadas por los administradores de sistemas y servicios, en el marco del cumplimiento normativo.

4.2. Analista técnico de datos

Este perfil debe llevar a cabo la explotación de la información contenida en diferentes repositorios y bases de datos de la ATM y de su protección. Trabajará en colaboración con el responsable de datos del Área de Sistemas e Innovación de la ATM.

Las actividades y funciones a realizar por este perfil, a título enunciativo que no limitativo, son los siguientes:

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

- Detección de datos sensibles
- Protección de los datos
- Creación de consultas en las diferentes bases de datos
- Creación de informes de uso y rendimiento de las bases de datos
- Explotación de las herramientas de BI (Business Intelligence)
- Revisión de regulaciones y afectaciones a ATM a nivel protección de los datos
- Diseño de la monitorización y auditoría de datos
- Documentación de la estructura de las bases de datos
- Gestión de tareas de informática forense

El analista técnico de datos deberá:

- Mantener la información del mapa de datos de los sistemas de información de la ATM.
- Colaborar con la definición de directrices y procedimientos para el cumplimiento de las políticas de los sistemas de información de la ATM, realizar su implementación, y monitorizar su aplicación.

4.3. Gestor documental de ciberseguridad.

Las actividades y funciones a realizar por este perfil, a título enunciativo que no limitativo, son los siguientes:

- Validación y mantenimiento de la política de gestión documental de ciberseguridad de la ATM.

- Modificación, actualización y mantenimiento del marco documental basado en la política de seguridad de la información.

- Establecimiento de roles y responsabilidades para la gestión de la documentación de seguridad.

- Identificación y clasificación de la información en función de su importancia, sensibilidad o criticidad.

- Definición del ciclo de vida de la información.

- Implementación de controles de versiones que garantice la correcta actualización y vigencia de los documentos y la información que éstos contienen.

- Establecimiento de los procesos de aprobación y acceso a los documentos y la información contenida.

- Validación y mantenimiento del contenido del Sistema de Gestión de la Seguridad de la Información (SGSI). El fondo documental estará principalmente en un repositorio organizado según los capítulos de un SGSI basado en el estándar ISO/IEC 27001.

4.4. Coordinador de la Oficina de Ciberseguridad.

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

Este perfil será el responsable de la coordinación de la Oficina de Ciberseguridad de la ATM dependiente del CISO.

Las actividades y funciones a realizar por este perfil, a título enunciativo que no limitativo, son los siguientes:

- Gestionar la gobernanza del marco normativo (políticas de seguridad, normas de seguridad, procedimientos de seguridad y otros de niveles jerárquicos inferiores), coordinación a nivel normativo de los diferentes departamentos que conforman la ATM o que tienen relación directa con éste, así como la gestión y alineamiento del marco normativo de los proveedores que suministran servicios y recursos tecnológicos a la ATM.
- Coordinar las acciones de adecuación normativa anteriormente descritas con el área legal de la ATM (Área de Asesoría Jurídica y Contratación) y la figura del Delegado de Protección de Datos (DPD) de la ATM.
- Coordinación y seguimiento de los proyectos de ciberseguridad de la ATM, así como de la operativa en materia de ciberseguridad.
- Responsable de los informes de seguimiento mensual de la Oficina de Ciberseguridad u otros informes que se le requieran.

Aparte de las tareas descritas en esta cláusula, el adjudicatario durante la ejecución del contrato se responsabilizará de las tareas de gestión, mejoras, ajustes y otros aspectos de gestión de la prestación que puedan surgir.

Los diferentes perfiles que componen la Oficina de Ciberseguridad de la ATM deberán velar por la colaboración con aquellos actores de actividades donde se requiera la participación de la Oficina.

Durante la ejecución del contrato, el adjudicatario deberá facilitar a la dirección de la contratación cualquier información solicitada con un plazo máximo de entrega de 5 días hábiles.

5. Finalidades y objetivos a alcanzar

La finalidad y objetivo que se debe alcanzar mediante la realización de este contrato es disponer de una Oficina de Ciberseguridad que en coordinación con el CISO, pueda establecer el marco ideal en la gestión de la ciberseguridad y la protección de los datos, que podrá dar respuesta y coordinar la necesidad de aumentar las herramientas de ciberseguridad y su explotación, el control de los datos de las organizaciones, así como la necesidad de adaptarse a las diferentes normativas como el ENS o a estándares como ISO.

6. Requerimientos técnicos generales obligatorios de la prestación

El adjudicatario dispondrá de los suficientes medios técnicos, materiales cualitativos y personales para desarrollar las tareas objeto de este contrato.

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

La prestación regulada en el presente pliego deberá ajustarse, al menos, a los siguientes requisitos técnicos, sin perjuicio de los parámetros a valorar mediante los criterios de adjudicación establecidos.

El adjudicatario deberá poner a disposición de la ATM durante el plazo de ejecución del contrato perfiles adecuados suficientemente cualificados, con la titulación correspondiente, formación y experiencia especializada en las materias que son objeto del contrato con los conocimientos necesarios para su correcto desarrollo, con los requisitos mínimos que se indican a continuación.

A continuación se identifican y se describen los diferentes perfiles a proporcionar por el adjudicatario, la responsabilidad y el porcentaje de horas de dedicación:

Perfil	Responsabilidades	Dedicación
Analista técnico de ciberseguridad	Tareas especificadas en el apartado 4.1	100%
Analista técnico de datos	Tareas especificadas en el apartado 4.2	100%
Gestor documental de ciberseguridad	Tareas especificadas en el apartado 4.3	50%
Coordinador de la Oficina de Ciberseguridad	Tareas especificadas en el apartado 4.4	75%

La experiencia profesional, titulación y conocimientos mínimos que se exige para este perfil son los siguientes:

Perfil	Titulación/ Experiencia/Conocimientos
Analista técnico de ciberseguridad	**Titulación:** Nivel grado en ingeniería informática o telecomunicaciones (o equivalente) **Experiencia:** Haber participado en un mínimo de 2 proyectos durante los últimos 2 años realizando tareas de técnico informático en tareas de explotación de herramientas de ciberseguridad. **Conocimientos:** Se valorarán otras titulaciones equivalentes y certificaciones en el sector de la ciberseguridad.
Analista técnico de datos	**Titulación:** Nivel grado en ingeniería informática y/o telecomunicaciones (o equivalente) **Experiencia:** Haber participado en un mínimo de 2 proyectos durante los últimos 2 años en gestión de datos. **Conocimientos:** Se valorará conocimiento en consultas en bases de datos (SQL), herramientas de BI e informes, monitorización y auditoría (Audit Vault – Oracle), así como otras titulaciones, certificaciones y experiencia en el ámbito de la explotación de los datos y de la ciberseguridad.
Gestor documental de ciberseguridad	**Titulación:** Nivel grado universitario

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

	Experiencia: Haber participado en un mínimo de 2 proyectos durante los últimos 2 años en gestión documental. **Conocimientos:** Se valorará conocimiento en estándares para la gestión documental como UNE-ISO 30301 y UNE-ISO 27001, o equivalentes.
Coordinador de la Oficina de Ciberseguridad	**Titulación:** Nivel grado en ingeniería informática o telecomunicaciones (o equivalente) **Experiencia:** Haber participado en un mínimo de 3 proyectos durante los últimos de 5 años en el ámbito de la gestión de la ciberseguridad, adecuación a marcos normativos como RGPD, ENS, PCI,... implementación de estándares ISO, NIST,... **Conocimientos:** Se valorará titulaciones, certificaciones y experiencia en el ámbito de la ciberseguridad y de la adecuación a normativas en la Administración Pública.

El adjudicatario deberá garantizar la continuidad de la prestación del servicio por parte del equipo durante todo el plazo de ejecución de los trabajos, previendo ausencias por causas planificadas o sobrevenidas. Cualquier cambio deberá ser autorizado previamente por la ATM. Los posibles cambios o modificaciones deberán ser comunicados por escrito a la ATM con la debida antelación y aceptados por la misma. En este supuesto el adjudicatario deberá proponer una/s persona/es con la formación y experiencia mínimas requeridas en la licitación, y en su caso, teniendo en cuenta las características de las personas valorado en la licitación, de acuerdo con su oferta.

Además, en caso de sustitución se exigirá lo siguiente:

- Un periodo de formación, a cargo del adjudicatario, por el nuevo miembro que se incorpore a la ejecución del contrato.
- Un periodo de coexistencia, de un mínimo de 15 días, entre la persona que causa baja y la persona que se incorpora.

La ATM se reserva la facultad de requerir al adjudicatario la sustitución cualquier perfil de la Oficina de Ciberseguridad con el fin de alcanzar un cumplimiento óptimo del contrato.

En este orden de cosas, se hace constar que la ATM queda desvinculada, a todos los efectos, de cualquier relación laboral con el personal de la entidad adjudicataria, dado que se trata de un contrato de apoyo y asistencia que debe ser considerado como tal en su conjunto.

La empresa contratista está obligada, en cuanto a estas personas, al cumplimiento de las disposiciones vigentes en materia laboral, de seguridad social y de seguridad y salud en el trabajo que le sean de aplicación.

La ejecución del contrato se interpreta como la prestación de un servicio y el contratista deberá garantizar la continuidad del mismo. Se llevará a cabo en las dependencias, calendario laboral y horario de la ATM y se coordinará con la empresa adjudicataria todas las cuestiones correspondientes a ausencias, periodos vacacionales, etc..,. Se

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

tendrá la posibilidad de ejecutar las jornadas laborales de forma presencial y teletrabajo, según requiera la ATM.

La ATM proporcionará a los componentes de la Oficina de Ciberseguridad las herramientas y los equipos informáticos necesarios para la realización del trabajo. De lo contrario, para el resto de perfiles los adjudicatarios deberán aportar los equipos informáticos necesarios para la prestación del servicio. Los componentes de la Oficina de Ciberseguridad dispondrán de teléfono móvil de contacto. La ATM no proporcionará el teléfono móvil ni el servicio de telefonía ni datos asociados al citado dispositivo. Tampoco asumirá ningún gasto de conectividad en el marco de trabajo fuera de las oficinas de la ATM en términos amplios dentro de la prestación del servicio contractual de referencia.

7. Formas de seguimiento y control de la ejecución de las condiciones.

El órgano de contratación designará a una persona que asumirá el control y la coordinación de la ejecución contractual con la empresa adjudicataria con el fin de tratar directamente las cuestiones relacionadas con el desarrollo normal de las tareas indicadas en este pliego.

El adjudicatario debe designar a una persona responsable a quien encargar la gestión de la ejecución del contrato y que deberá garantizar la calidad de la prestación objeto de este pliego, tratando directamente las cuestiones relacionadas con el desarrollo normal de las tareas indicadas en este pliego con la persona interlocutora designada por el órgano de contratación.

8. Calendario de trabajo y duración del contrato

Se establece una duración del presente contrato de los meses correspondientes entre la fecha de inicio del contrato y la fecha de finalización del mismo, fijada el 20 de junio de 2026, para la prestación de los servicios objeto de este pliego.

Dentro de los 10 días siguientes a la fecha de inicio de la prestación del objeto del contrato, la empresa contratista deberá entregar al responsable del contrato el programa de trabajo para su aceptación. La dirección del contrato resolverá sobre el programa de trabajo dentro de un plazo de 5 días contados a partir de la fecha de entrega, entendiéndose que la resolución podrá introducir modificaciones, siempre que no contravengan las condiciones del contrato.

9. Condiciones generales de ejecución y ciberseguridad

9.1. Principios básicos

- **Deber de confidencialidad.** El personal de la empresa adjudicataria debe mantener absoluta confidencialidad y estricto secreto sobre la información conocida a raíz de la

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

ejecución de los servicios contratados. Esta obligación de confidencialidad tiene carácter indefinido y subsistirá incluso después de haber cesado su relación laboral con la ATM. La empresa adjudicataria debe comunicar esta obligación de confidencialidad a su personal y debe controlar su cumplimiento. La empresa adjudicataria debe poner en conocimiento de la ATM, de forma inmediata, cualquier incidencia que se produzca durante la ejecución del contrato que pueda afectar a la integridad o la confidencialidad de la información. Este deber se extiende a los empleados de otras empresas que, a petición del adjudicatario, participen en la prestación de los servicios recogidos en este pliego.

- **Propiedad intelectual**: toda la documentación que se genere durante la prestación de los servicios de apoyo es propiedad exclusiva de la ATM.

  Toda la documentación generada en la presente contratación será propiedad de la ATM y no se podrá hacer ningún uso por parte del Adjudicatario, así como todos los desarrollos realizados dentro de la presente licitación.

- **Criterios de accesibilidad universal:** la empresa adjudicataria se responsabilizará de cumplir con los criterios de accesibilidad universal, tal y como son definidos estos términos en el texto refundido de la Ley General de derechos de las personas con discapacidad y de inclusión social, aprobado mediante Real Decreto Legislativo 1/2013, de 29 de noviembre.

  Los medios de comunicación, el diseño de los elementos instrumentales y la implantación de los trámites procedimentales empleados por la empresa contratista en la ejecución del contrato deberán realizarse teniendo en cuenta los criterios de accesibilidad universal y de diseño para todos.

- **Criterios de sostenibilidad y protección al medio ambiente: la** empresa adjudicataria se responsabilizará de cumplir los criterios de sostenibilidad y protección del medio ambiente, de acuerdo con las definiciones y principios regulados en los artículos 3 y 4, respectivamente, del *Real Decreto Legislativo 1/2016, de 16 de diciembre, por el que se aprueba el texto refundido de la Ley de prevención y control integrados de la contaminación*.

  Siempre que sea posible, la empresa contratista deberá hacer una elección inteligente de materiales (uso de materiales adecuados para el medio ambiente, evitando los que no lo sean), equipos de eficiencia energética (reducir el coste energético y la huella de carbono colectivo), final de la vida útil y reutilización, etc.

9.2. Marco de cumplimiento normativo

El actual marco normativo para las entidades públicas de Catalunya, está establecido, principalmente, en la Política de Ciberseguretat de la Generalitat de Catalunya de septiembre del 2021. Esta política recoge directivas y reglamentos del Parlamento y Consejo Europeo, reales decretos del estado español, así como instrucciones de la Generalitat de Catalunya. Este marco de cumplimiento normativo en temas de ciberseguridad y protección de datos, abarca a las entidades públicas de la Generalitat de Catalunya y a todos aquellos que participan en la prestación de sus servicios.

9.2.1. Datos de carácter personal.

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

El adjudicatario tratará los datos de carácter personal a que acceda como consecuencia de la ejecución de este contrato de conformidad con lo establecido en la normativa vigente en la materia.

La empresa adjudicataria se responsabilizará del uso adecuado de la información que se pueda obtener con el fin de proteger los datos personales, a lo largo de toda la fase de realización del objeto del contrato y también una vez finalizada sobre la base de las normativas internacionales al respecto y de obligado cumplimiento, entre ellos y expresamente, el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, sobre la protección de las personas físicas con respecto al tratamiento de datos personales y a la libre circulación de los datos mencionados, así como cualquier otra normativa nacional y de la Unión Europea que sea aplicable en materia de protección de datos y en relación con los datos personales a que tiene acceso durante la vigencia de este contrato.

El incumplimiento de estas obligaciones constituye la infracción tipificada en la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales, sin perjuicio de las responsabilidades exigidas ante la jurisdicción ordinaria.

El Adjudicatario con relación a aquellos datos que por la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) sea necesario, en la solución propuesta lo ha cumplido, p. ej. ubicar los datos en una base de datos física diferente, cifrar los datos, control de acceso, etc.

El Adjudicatario se compromete a cumplir, con relación a los datos tratados en la ejecución del presente contrato:

La Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).

las buenas prácticas para la gestión de la seguridad de la información

9.2.2. Esquema Nacional de Seguridad (ENS)

El artículo 2 del vigente Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, dispone que los pliegos de prescripciones administrativas o técnicas de los contratos que celebren las entidades del sector público incluidas en el ámbito de aplicación del real decreto del ENS contemplarán todos aquellos requisitos necesarios para asegurar la conformidad con el mismo de los sistemas de información en los que se sustenten los servicios prestados por los contratistas, como la presentación de las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS. Esta cautela se extenderá también a la cadena de servicios de estos contratistas, en la medida en que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos.

La ATM, considera necesario que los proveedores que vayan a concurrir a esta licitación deberán estar en condiciones de exhibir una Declaración de Conformidad con el ENS. Así pues, en base a lo anterior, y al análisis de los riesgos a los que están expuestos los servicios objeto de la licitación, la ATM establece como necesario que las entidades licitadoras deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad, así como mantener la conformidad en vigor durante la vigencia del contrato. Esta declaración de conformidad con la ENS debe abarcar el ámbito objeto de la contratación.

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

Por otra parte, se ha establecido como criterio objetivo de valoración de las ofertas el disponer por parte de los licitadores de un nivel superior de conformidad al Esquema Nacional de Seguridad, de manera que el licitador adjudicatario deberá mantener el nivel declarado durante todo el plazo de ejecución del contrato.

En el caso de que el adjudicatario no pudiera mantener la conformidad con el ENS durante la vigencia del contrato -por imposibilidad de mantener la Declaración de Conformidad o pérdida, retirada o suspensión de la Certificación de Conformidad-, deberá comunicar esta circunstancia, de manera inmediata y sin dilación indebida, a la ATM, quien considerará el impacto de esta circunstancia en la prestación objeto del contrato.

Se establece un mecanismo provisional de acreditación de cumplimiento con la ENS, que consiste con la posibilidad de los proveedores de presentar informes de auditoría, declaraciones de aplicabilidad o procesos de certificación en curso, la aceptación de estos documentos dependerá de la validación por parte de la ATM.

Se valorará un mayor nivel del cumplimiento del ENS por encima del mínimo requerido.

Los requerimientos de este marco de cumplimiento normativo no excluyen otros requerimientos de ciberseguridad que puedan estar incluidos en este pliego.

9.3. Seguimiento

El adjudicatario asignará un responsable de seguridad y protección de datos para tratar los temas de ciberseguridad. El adjudicatario entregará durante la ejecución del contrato un modelo de seguimiento de la ciberseguridad en función de la fase del proyecto.

Este responsable podrá coincidir con el perfil del Coordinador de la Oficina de Ciberseguridad ofrecido por el adjudicatario.

10. Documentación técnica que deben aportar las empresas licitadoras

Las especificaciones técnicas propuestas por la empresa licitadora en su oferta se convertirán en condiciones de obligado cumplimiento a lo largo de la ejecución del contrato si ésta se convierte en la adjudicataria.

El licitador deberá presentar una propuesta técnica de acuerdo con el modelo del anexo 1 del PCA, que incluirá en todo caso:

- Descripción de los diferentes perfiles de la Oficina de Ciberseguridad que pondrán a disposición del contrato, que incluya la titulación, formación, conocimientos y experiencia del equipo de trabajo, que debe cumplir con los requerimientos mínimos establecidos en este Pliego.
- La propuesta técnica deberá incluir una descripción de la metodología de trabajo que propone el licitador para el desarrollo del servicio teniendo en cuenta la sistemática que utilizará para llevar a cabo la prestación con las especificidades particulares que garanticen su correcta ejecución e interrelación con la ATM.
- Será necesario que se incluya la descripción de la metodología en cuanto al control y seguimiento del equipo, la descripción del control y seguimiento del servicio así como

Balmes, 49 6a planta
08007 Barcelona
atm@atm.cat
www.atm.cat

de las herramientas de gestión que se emplearán para la realización de los servicios a contratar.

Carme Fàbregas Casas
Directora de l'Àrea de Sistemes i Innovació

Signat electrònicament